## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
## BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | | |
|---|---|---|
| In re Application of: | § | Filed: July 24, 2003 |
| Lewis et al. | § | |
| | § | Group Art Unit: 2134 |
| Serial No.: 10/625,955 | § | |
| | § | Examiner: Matthew E. Heneghan |
| Confirmation No.: 1644 | § | |

For: METHOD TO DISABLE ON/OFF CAPACITY ON DEMAND

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**CERTIFICATE OF MAILING OR TRANSMISSION**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office to fax number 571-273-8300 to the attention of Examiner Matthew E. Heneghan, or electronically transmitted via EFS-Web, on the date shown below:

| | |
|---|---|
| February 21, 2008 | /Jon K. Stewart/ |
| Date | Jon K. Stewart |

## APPEAL BRIEF

Dear Sir:

Applicants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2134 dated September 21, 2007, finally rejecting claims 1-17 and 20-53. The final rejection of claims 1-17 and 20-53 is appealed. This Appeal Brief is believed to be timely since it is transmitted by the due date of February 21, 2008, as set by the filing of a Notice of Appeal on December 21, 2007.

Please charge the fee of $510.00 for filing this brief to:

Deposit Account No. 09-0465 / ROC920030175US1.

# TABLE OF CONTENTS

## Real Party in Interest

The present application has been assigned to International Business Machines Corporation, Armonk, New York.

## Related Appeals and Interferences

Applicant asserts that no other appeals or interferences are known to the Applicant, the Applicant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

## Status of Claims

Claims 1-17 and 20-53 are pending in the application. Claims 1-53 were originally presented in the application. Claims 18-19 have been canceled without prejudice. Claims 1-17 and 20-53 stand finally rejected as discussed below. The final rejections of claims 9-17 and 20-53 are appealed. The pending claims are shown in the attached Claims Appendix.

## Status of Amendments

All claim amendments have been entered by the Examiner, including amendments to the claims proposed after the final rejection.

## Summary of Claimed Subject Matter

Claimed embodiments include methods (*see claims* 9-17 and 20-35), computer programs stored on computer readable storage media (*see claims* 36-46) and computer systems (*see claims* 47-53) directed to the selective enablement and disablement of hardware capacity on a computerized apparatus. *See Application*, 1:15-17, 7:6-11, Abstract.

### A. CLAIM 9 – INDEPENDENT

Claim 9 recites a method for disabling on-demand resources on a computerized apparatus. *See Application*, 1:15-17, 4:11-19, 7:6-11, Figure 4, 400. As claimed, this method includes receiving a disablement code comprising encrypted data. *See Application*, 15:9-16, 15:21-25, Figure 3, 115, Figure 4, 402. And also includes validating the disablement code. *See Application*, 11:21-30, 12:1-2, 16:5-8, Figure 4, 414, Figure 5, 500. As recited by Claim 1, the validating step includes generating a first key using system information unique to the computerized apparatus. *See Application*, 16:13-15, Figure 5, 502. Regarding the system information, see Application, 10:1-19 and 13:20-27. As claimed, the validating also includes decrypting the encrypted data using a second key to produce decrypted data, *see Application*, 16:26-30, Figure 5, 508, and encrypting a value to produce an encrypted value wherein the encrypting is done using an encryption key selected from one of (i) the decrypted data and (ii) the first key. *See Application*, 17:11-17, Figure 5, 513, 515, et seq. As claimed, the validating further includes decrypting the encrypted value to produce a decrypted value wherein the decrypting is done using (i) the first key if the value was encrypted using the decrypted data as the encryption key and (ii) the decrypted data if the value was encrypted using the first key as the encryption key. *See Application*, 17:17-35, Figure 5, 520, 522, 528, et seq. The validating also includes comparing the value to the decrypted value*.* *See Application*, 17:17-35, Figure 5, 520, 522, 528, et seq. The method recited by claim 1 includes disabling at least one on-demand resource if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, et seq. Also as claimed, the disabled on-demand resource is a hardware resource of the computerized apparatus. *See Application*, 13:5-13.

## B. CLAIM 20 - INDEPENDENT

Claim 20 recites a method for controlling availability of on-demand resources on a computerized apparatus. *See Application*, 1:15-17, 4:21-28, 7:6-11, Figure 4, 400, Figure 5, 500. This method includes receiving an enablement code for an on-demand resource, *see Application*, 11:4-18, 13:5-13; validating the enablement code, *see Application*, 11:21-30, 12:1-6; and enabling the on-demand resource, whereby usage of the on-demand resource may be requested by a user. *See Application*, 12:8-30. As claimed, this method also includes receiving a disablement code for an on-demand resource. *See Application*, 11:4-8, 13:1-3, 15:9-16, 15:21-25, Figure 3, 115, Figure 4, 402. Aspects of disablement codes are also discussed at Application, 9:14-29 and 10:1-19. This method also includes validating the disablement code. *See Application*, 11:21-30, 12:1-2, 16:5-8, Figure 4, 414, Figure 5, 500. And also includes disabling the on-demand resource. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, et seq. As claimed, the disabled on-demand resource is a hardware resource of the computerized apparatus, whereby usage of the on-demand resource may no longer be requested by the user. *See Application*, 13:5-13, 15:9-16, Figure 3, 115.

## C. CLAIM 31 - INDEPENDENT

Claim 31 recites a method for generating disablement codes for disabling on-demand resources on a computerized apparatus. *See Application*, 1:15-17, 4:30-32, 5:1-6, 7:6-11, 8:12-25, Figure 4, 400. As claimed, this method includes inputting a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus. *See Application*, 13:1-3, 11:4-8, 11:21-30 9:14-29, 10:1-19, 13:5-13. This method also includes outputting an authentication code, *see Application*, 13:22,-17, 14:1-9, Figure 2, and includes encrypting the authentication code. *See Application*, 14:23-28, 15:1-7, 17:11-17, Figure 5, 513, 515. This method also includes providing a disablement code to a user of the computerized apparatus, the disablement code comprising the encrypted authentication code and being configured to disable an on-demand resource on the computerized apparatus upon being validated, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, 15:9-16, Figure 3, 115. As claimed, the disabled on-demand resource is a hardware resource of the computerized apparatus. *See Application*, 13:5-13.

## D. CLAIM 36 - INDEPENDENT

Claim 36 is directed to a computer readable medium containing a program which, when executed, performs an operation for generating disablement codes for disabling on-demand resources on a computerized apparatus. *See Application* 1:15-17, 7:6-11, 5:8-17, 7:17-39. As claimed, the operation includes receiving a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus, *see Application*, 13:1-3, 11:4-8, 11:21-30 9:14-29, 10:1-19, 13:5-13; outputting an authentication code, *see Application*, 13:22,-17, 14:1-9, Figure 2; and also includes encrypting the authentication code; and outputting a disablement code for the computerized apparatus. *See Application*, 14:23-28, 15:1-7, 17:11-17, Figure 5, 513, 515. As claimed, the disablement code comprising the encrypted authentication code and being uniquely configured to disable an on-demand resource on the computerized apparatus upon being validated, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, 15:9-16, Figure 3, 115. Also as claimed, the disabled on-demand resource is a hardware resource of the computerized apparatus. *See Application*, 13:5-13.

## E. CLAIM 38 - INDEPENDENT

Claim 38 is directed to a computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus. *See Application* 1:15-17, 5:19-30, 6:1-2, 7:6-11, 7:17-39. As recited by claim 38, the operation includes receiving the disablement code comprising encrypted data, *see Application*, 15:9-16, 15:21-25, Figure 3, 115, Figure 4, 402, and validating the disablement code. *See Application*, 11:21-30, 12:1-2, 16:5-8, Figure 4, 414, Figure 5, 500. As recited by claim 38, the validating operation includes generating a first key using system information unique to the computerized apparatus. *See Application*, 16:13-15, Figure 5, 502. Regarding the system information, see Application, 10:1-19 and 13:20-27. The validating operation also includes sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key. *See Application*, 16:26-30, 17:1-9, Figure 1, 130, Figure 5, 506. This operation also includes generating a random value, *see Application*, 17:11-14, Figure 5, 513, and encrypting the random value using the first key to produce an encrypted random value. *See Application*, 17:14-17, Figure 5, 515. The validation operation also includes sending the encrypted random value to the secure storage element, wherein the secure storage element is configured to decrypt the encrypted random value, using the decrypted data as a decryption key, to produce a decrypted random value. See Application, Figure 1, 130, 17:16-18, Figure 5, 516, 518. The validation operation also includes receiving the decrypted random value from the secure storage element. *See Application*, 17:19-20, Figure 5, 520. The operation for validating the disablement code also includes comparing the value to the decrypted random value. *See Application*, 17:20-26, Figure 5, 522, 524, 526, and 528.

## F. CLAIM 46 - INDEPENDENT

Claim 46 is directed to a computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus. *See Application* 1:15-17, 5:19-30, 6:1-2, 7:6-11, 7:17-39. As recited by claim 46, the operation includes receiving the disablement code comprising encrypted data, *see Application*, 15:9-16, 15:21-25, Figure 3, 115, Figure 4, 402, and validating the disablement code. *See Application*, 11:21-30, 12:1-2, 16:5-8, Figure 4, 414, Figure 5, 500. As recited by claim 38, the validating operation includes generating a first key using system information unique to the computerized apparatus. *See Application*, 16:13-15, Figure 5, 502. The validating operation also includes sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key and further configured to encrypt a value using the decrypted data as an encryption key. *See Application*, Figure 1, 130, 16:26-30, 17:1-9, Figure 5, 506, 17:16-18, Figure 5, 516, 518. As recited by claim 46, the validation operation also includes receiving the encrypted value from the secure storage element. *See Application*, 17:19-20, Figure 5, 520, and includes decrypting the encrypted value using the first key. *See Application*, Figure 1, 130, 16:26-30, 17:1-9, Figure 5, 506, 17:16-18, Figure 5, 516, 518. The operation for validating the disablement code also includes disabling the on-demand resources if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, 15:9-16, Figure 3, 115. Also as claimed, the disabled on-demand resource is a hardware resource of the computerized apparatus. *See Application*, 13:5-13.

## G. CLAIM 47 - INDEPENDENT

Claim 47 is directed to a computerized apparatus. *See Application* 1:15-17, 6:4-10, 8:12-25. As claimed, the apparatus includes a plurality of resources at least one of which comprises an on-demand resource configured to be requested by a user once enabled. *See Application*, 13:5-13. The apparatus also includes a capacity manager. *See Application*, 9:14-25, Figure 1, 120. As claimed, the capacity manger is configured to receive an enablement code for the on-demand resource, *see Application*, 11:4-18, 13:5-13, and to enable the on-demand resource. *See Application*, 12:8-30. As claimed, the capacity manger is further configured to receive a disablement code for the on-demand resource. *See Application*, 11:4-8, 13:1-3, 15:9-16, 15:21-25, Figure 3, 115, Figure 4, 402. Aspects of disablement codes are also discussed at Application, 9:14-29 and 10:1-19. The capacity manger is further configured to validate the disablement code. *See Application*, 11:21-30, 12:1-2, 16:5-8, Figure 4, 414, Figure 5, 500. And to disable the on-demand resource, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus. *See Application*, 16:5-8, Figure 4, 416, 418, 17:23-26, Figure 5, 526, et seq. Additionally, the disabled on-demand resource is a hardware resource of the computerized apparatus. *See Application*, 13:5-13, 15:9-16, Figure 3, 115.

## Grounds of Rejection to be Reviewed on Appeal

1. The rejection of claims 9-17 and 20-53 under 35 U.S.C. § 103(a) as being unpatentable over *MacKenzie et al.*, U.S. Pat. No. 7,149,311 (hereinafter *MacKenzie*) in view of *Silver et al.*, U.S. Pat. No. 6,975,204 (hereinafter *Silver).*

## ARGUMENTS

### 1. Claims 9-17 and 20-53 are not Obvious over *MacKenzie* in View of *Silver.*

*The Applicable Law*

The Examiner bears the initial burden of establishing a *prima facie* case of obviousness. *See* MPEP § 2142. To establish a *prima facie* case of obviousness three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one ordinary skill in the art to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP § 2143. The present rejection fails to establish at least the third criteria.

For example, *MacKenzie* in view of *Silver*, does not disclose a "method for disabling on-demand resources on a computerized apparatus" that includes "disabling at least one on-demand resource if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus," as recited by claim 9. Independent claims 20, 31, 36, 38, 46, and 47 each recite a similar limitation.

*MacKenzie* discloses a technique for protecting access to a cryptographic "private key," part of a key pair that includes both a "private key" and a "public key." Ultimately, the keys are just very large, but related numbers. As is well known, a "private key" provides one of two keys used in asymmetric cryptography. The private key can be used to decrypt data that has been encrypted using the public key, which is shared with all involved parties. The private key is also used to "sign" outgoing messages. "Signing" typically involves encrypting the message (or a hash of the message) using the private key. Because the public key is shared, anyone can then decrypt the message (or the hash) to verify that the message was, in fact, "signed" with the private key. So long as you believe the private key is possessed only by a particular person, you can rely on this to believe that any messages signed with the private key were, in fact, sent by the particular person.

Of course, because the private key can be used in this manner to "sign" messages, a compromised key may be used impersonate the rightful key-holder. Similarly, a comprised private key may be used to access messages, documents, etc. encrypted with the corresponding public key. As stated ultimately, the private key and public key are simply two large numbers related to one another in a particular way. Also, the private key and public key are typically represented as hexadecimal values.

Because of the obvious security issues related to the private key, and possible consequences that flow from unwanted disclosure, a number of techniques have been developed to safeguard the security thereof. For example, the private key is usually encrypted with an asymmetric key, i.e., a key that may be used to both encrypt and decrypt information. Typically, the asymmetric key is expressed as a user password. However, this leaves the private key open to a "dictionary attack," i.e., an attack of simply guessing every possible password until finding the correct one.

Regarding claims 9, 36, and 46:

Against this background of well understood cryptographic techniques, *MacKenzie* discloses a technique for "key disabling," by which "the rightful owner of a stolen device can disable the device's private key even if the attacker already knows the user's password." *Mackenzie*, Abstract. That is, *MacKenzie* discloses a means to revoke a compromised private key, to prevent the use of a revoked key in cryptographic operations.

In rejecting claim 9, 36, and 46, the Examiner suggests:

> As per claims 9, 10, 17, 36, and 46, an algorithm is disclosed in which a verification is performed by decrypting the command to get a value b, and also generates a field y, which it then decrypts to derive a value ß. If ß does not equal beta the disablement operation is aborted by stopping further decryption of it (see column 16, lines 9-38); otherwise, the operation continues.

*Final Office Action*, p. 3. The passage cited by the Examiner provides:

> In step 302, the well-formedness of the ciphertext c is tested by the device. If the function valid(c) returns a zero, the decryption protocol is aborted. If the function valid(c) returns a one, the decryption protocol continues on to the next steps. As before, the device computes ß in step 304, which is a value that proves the device's knowledge of $\pi$ to the server. The device computes $\rho$ in step 306. As before, $\rho$ is a one-time pad by which the server encrypts certain values (in this case, v, e, s) to return them to the device after performing its share of the decryption operations. In step 308, the device computes $\gamma$, which is an encryption of c, ß, and $\rho$, to securely transport these values to the server. In step 310, the device also computes value $\delta$, which is a message authentication code computed using a, to show the server that this request originated from the device.
>
> Next, in step 312, the device transmits the values $\gamma$, $\delta$ and $\tau$ to the server.
>
> Upon receipt of these values, the server decrypts the ticket $\tau$ in order to recover values a, b, u, p, q, g and $x_2$ in step 314. As before, in step 316, the server uses . $\gamma$, $\delta$, and $\tau$ to confirm that this request for a private key actually originated from the device. Thus, if $mac_a(<\gamma,\tau>) \neq \delta$ , then the server aborts the decryption operation. In step 318, the server decrypts $\gamma$ in order to recover values c, ß, and $\rho$. In step 320, the server determines whether it is in receipt of a request that bears $\tau$ and originated from the device, but that it is a request for which the device's knowledge of the user's password cannot be verified. Thus, if, ß. $\neq$ b, then the server aborts the decryption operation.

*MacKenzie*, 16:9-38. The passage cited by the Examiner describes steps of a method spelling out a "protocol 300 with key disabling in accordance with a second embodiment of the present invention, i.e., the D-ELG protocol." *MacKenzie*, 15:65-67. The "D-ELG" protocol refers to the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement developed in 1985, and as "described in T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, 31:469 472, 1985." *See MaKenzie*, 14:59-63. The ElGamal cryptosystem provides an implementation of the more general public key encryption techniques discussed above.

The passage cited by the Examiner describes how the ElGamal cryptosystem may be used to decrypt "a ciphertext c generated using the device's public key in an ElGamal-like encryption scheme. The input provided to the device for this protocol is the input password $\pi$, the ciphertext c, and all the values saved on stable storage in the initialization protocol of subsection 2.2.1. See *MacKenzie*, 16:1-7. Stripped of some of the complexity, the steps include:

- Device tests whether the message a well formed ciphertext, the ciphertext includes a request for access to a private key. (step 302) See *MacKenzie*, 16:9-12.
- If so, device computes ß, where ß is the hash of a password input to the decryption operation (step 304). See *MacKenzie*, 10:24-27, Figure 1, 102, 16:4-6.
- Device computes ρ, a one-time pad used to encrypt ciphertext c, returned to a device. See *MacKenzie*, 10:27-28, Figure 1, 104. (step 306)
- Device computes γ as an encryption of ciphertext c, ß and ρ. (Step 308)
- Device computes δ as message authentication code. (step 310)
- Device transmits computed values to server. (Step 312)
- Server verifies the authenticity of the request:
  - First, server decrypts τ (step 314) to confirm that this request for a private key originated from the device (step 316), i.e., the request is from the authorized device.
  - Second, server decrypts γ to recover ciphertext c, ß, and ρ (step 318).
- Server verifies that the request originated from the device but the device's knowledge of the user's password cannot be verified. (step 320).

Applicants submit that this extremely detailed and narrow cryptographic protocol disclosed in *MacKenzie* for validating a request for a private key based on whether (i) the request originating from a particular device and (ii) whether the device has knowledge of the user's password fails to disclose a "method for disabling on-demand resources on a computerized apparatus" that includes receiving and validating a disablement code in the manner claimed. No "disablement code" used to disable access to an "on-demand" resource, where the on-demand resource is a hardware resource of the computerized apparatus," as recited by claim 9. In fact, the Examiner does not even argue a mapping from these steps of the method disclosed in *MacKenzie* to the limitations of the present claims. Instead, the Examiner rejects the complete claim by making the sweeping conclusion that "If ß does not equal beta the disablement operation is aborted by stopping further decryption of it (see column 16, lines 9-38)." *Final Office Action*, p. 3. However, the decryption operation from *MacKenzie* does not disclose a "disablement operation," at all. Instead, it discloses steps of the *ElGamal* cryptosystem used to validate a request for access to a private key.

Similarly, Applicants submit that the decryption protocol of the ElGamal decryption system disclosed in *MacKenzie* discloses "a computer readable medium containing a program which, when executed, performs an operation for generating disablement codes for disabling on-demand resources on a computerized apparatus," as recited by claim 46. In particular, where the operation includes "receiving a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus," as recited by claim 36. And also fails to disclose a computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus," as recited by claim 46, In particular, where operation includes validating the disablement code, the validating itself including generating a first key using system information unique to the computerized apparatus, and includes sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key and further configured to encrypt a value using the decrypted data as an encryption key.

Furthermore, Applicants submit that *MacKenzie* in view of *Silver*, does not disclose a "method for disabling on-demand resources on a computerized apparatus" that includes "disabling at least one on-demand resource of the computerized apparatus, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus," as recited by claims 9. Independent claims 20, 31, 36, 46, and 47 each recite a similar limitation.

Regarding this limitation, the Examiner suggests:

> As per claims 1, 8, and 31, *MacKenzie* discloses the disabling of a key-utilizing resource via an encrypted user disablement command generated from inputted authorization codes issued via a remote server, which is executed after it is verified (authenticated) (see column 6, lines 43-48).

*Final Office Action*, p. 2. The passage cited by the Examiner provides:

> In the key disabling type of protocol of the invention, the user can issue a request to the server to disable future use of the private key associated with the device's public key. Once the server receives this request and verifies it is well-formed, the device's key is rendered useless to the attacker, even if the attacker knows the user's password.

*MacKenzie*, 6:43-48. Stated differently, once the server verifies a request to revoke a private key, the server will refuse to allow the use of that key (e.g., for message signing and decrypting). Note, the cryptographic mathematics still function using both the password and the private key, but the server will nevertheless refuse to use the private key in any requested cryptographic operations.

Based on the foregoing, it should be clear that *Mackenzie* does not disclose "disabling at least one on-demand resource, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus." Rather, *MacKenzie* discloses a technique for revoking the validity of a private key, of a private public key pair, in order to prevent a comprised private key from being used in cryptographic operations "even if the attacker knows the user's password." Thus, no "on-demand resources on a computerized apparatus" are disabled in the private-key revocation process disclosed in *MacKenzie.*

Further still, in rejecting claim 20, the Examiner suggests:

> As per claim 20, 22, and 25-28, the resource is enabled (i.e. unlocked) during initialization via the appropriate codes before disablement (see column 13, line 10 to column 14, line 56).

Final Office Action, p. 3. However, Applicants submit that *MacKenzie* fails to disclose "a method for controlling availability of on-demand resources on a computerized apparatus," as recited by claim 20. In particular, *MacKenzie* does not disclose a method that includes "receiving an enablement code for an on-demand resource; validating the enablement code; and enabling the on-demand resource, whereby usage of the on-demand resource may be requested by a user."

Instead, the passage cited by the Examiner describes aspects of a "device initialization process." The initialization process is used to set up a system to "communicate by exchanging messages over a public network." *See MacKenzie*, 6:62-66. As disclosed in Mackenzie, the "system is initialized with public data, secret data for the device, secret data for the user of the device (i.e., $\pi_0$), and secret data for the server. The public and secret data associated with the server may simply be a certified public key and associated private key, respectively, which is set up well before the device is initialized." In other words, the "initialization process" is an exchange of cryptographic data between the server and the device that occurs prior to "the device" being used "either for generating signatures or decrypting messages (i.e., private key operations)," *MacKenzie*, 7:1-10. At the same time, Applicants submit that nothing in this "initialization process" discloses the claimed step of "receiving an enablement code for an on-demand resource; validating the enablement code; and enabling the on-demand resource, whereby usage of the on-demand resource may be requested by a user," as recited by claims 20, 22, and 25-28.

Further still, in rejecting claim 38, the Examiner suggests:

> Regarding claim 38, 41, 42, and 45, the authentication may also include the verification of the transmission of random numbers (see column 10, lines 37-53, which is also. incorporated into the disablement protocol).

*Final Office Action*, p. 3. Claim 38 is directed to a program configured to perform "an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus," that includes:

> generating a random value;
> encrypting the random value using the first key to produce an encrypted random value;
> sending the encrypted random value to the secure storage element, wherein the secure storage element is configured to decrypt the encrypted random value, using the decrypted data as a decryption key, to produce a decrypted random value;
> receiving the decrypted random value from the secure storage element; and
> comparing the value to the decrypted random value.

In contrast, the passage describes how a particular type of denial-of-service attack may be avoided by including a time-out period:

> On the contrary, if this former category were treated like the latter, then this would enable a denial-of-service attack on .tau. (i.e., the device) in which an attacker, having seen .$\tau$, $\gamma$, and $\delta$. pass on the network, submits requests to the server containing $\tau$ and random values for $\gamma$ and $\delta$.

*MacKenzie*, 10:49:53. Applicants submit that the passage cited by the examiner does not disclose a process for validating a disablement code that includes "generating a random value and encrypting the random value using the first key to produce an encrypted random value." Instead, the passage points out an attack where random values are supplied to a server as part of a denial of service attack.

For all the foregoing reasons, Applicants submit that claims 9, 20, 31, 36, 38, 46, 47, and the claims dependent therefrom are not rendered obvious by *MacKenzie* in view of *Silver*. Accordingly, Applicants respectfully request that the rejection of these claims be vacated by the Board.

## CONCLUSION

The Examiner errs in finding that claims 9-17 and 20-53 are unpatentable over *MacKenzie* in view of *Silver* under 35 U.S.C. § 103(a).

Withdrawal of the rejections and allowance of all claims is respectfully requested.

Respectfully submitted, and
**S-signed pursuant to 37 CFR 1.4,**

/Gero G. McClellan, Reg. No. 44,227/

Gero G. McClellan
Registration No. 44,227
Patterson & Sheridan, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846
Attorney for Appellant(s)

## CLAIMS APPENDIX

1. (Previously Presented) A computer-implemented method for disabling on-demand resources on a computerized apparatus, comprising:

receiving a disablement code;

validating the disablement code; and

disabling at least one on-demand resource, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

2. (Original) The computer-implemented method of claim 1 wherein validating comprises encrypting and decrypting data.

3. (Original) The computer-implemented method of claim 1 wherein validating comprises verifying that the disablement code is unique to the at least one on-demand resource.

4. (Original) The computer-implemented method of claim 1 wherein the at least one on-demand resource was previously enabled to allow a user to request usage of the at least one on-demand resource.

5. (Original) The computer-implemented method of claim 1 wherein prior to disabling, the at least one on-demand resource is enabled to allow a user to request usage of the at least one on-demand resource; and wherein disabling the at least one on-demand resource comprises preventing the user from requesting usage of the at least one on-demand resource.

6. (Original) The computer-implemented method of claim 1 wherein the at least one on-demand resource is a processor.

7. (Original) The computer-implemented method of claim 1 wherein the at least one on-demand resource comprises one of memory and storage.

8. (Original) The computer-implemented method of claim 1 wherein the disablement code is input by a user.

9. (Previously Presented) A computer-implemented method for disabling on-demand resources on a computerized apparatus, comprising:

receiving a disablement code comprising encrypted data;

validating the disablement code, the validating comprising:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value to produce an encrypted value wherein the encrypting is done using an encryption key selected from one of (i) the decrypted data and (ii) the first key;

decrypting the encrypted value to produce a decrypted value wherein the decrypting is done using (i) the first key if the value was encrypted using the decrypted data as the encryption key and (ii) the decrypted data if the value was encrypted using the first key as the encryption key; and

comparing the value to the decrypted value; and

disabling at least one on-demand resource if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

10. (Original) The computer-implemented method of claim 9 wherein the validating is successful if the value and the decrypted value are the same.

11. (Original) The computer-implemented method of claim 9 wherein the decrypted data is identical to the first key.

12. (Original) The computer-implemented method of claim 9 wherein decrypting the encrypted data is performed by a smart chip containing the second key.

13. (Original) The computer-implemented method of claim 9 wherein the at least one on-demand resource was previously enabled to allow a user to request usage of the at least one on-demand resource.

14. (Original) The computer-implemented method of claim 9 wherein, prior to the disabling, the at least one on-demand resource is enabled to allow a user to request usage of the at least one on-demand resource and wherein disabling comprises preventing the user from requesting usage of the at least one on-demand resource.

15. (Original) The computer-implemented method of claim 9 wherein the at least one on-demand resource is a processor.

16. (Original) The computer-implemented method of claim 9 wherein the at least one on-demand resource comprises one of memory and storage.

17. (Original) The computer-implemented method of claim 9 wherein the disablement code is input by a user.

18 - 19. (Canceled)

20. (Previously Presented) A computer-implemented method for controlling availability of on-demand resources on a computerized apparatus, comprising:

receiving an enablement code for an on-demand resource;

validating the enablement code;

enabling the on-demand resource, whereby usage of the on-demand resource may be requested by a user;

receiving a disablement code for an on-demand resource;

validating the disablement code; and

disabling the on-demand resource, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus; whereby usage of the on-demand resource may no longer be requested by the user.

21. (Original) The computer-implemented method of claim 20 wherein validating the enablement code and validating the disablement code are performed by the same algorithm.

22. (Original) The computer-implemented method of claim 20 wherein enabling comprises unlocking the on-demand resource.

23. (Original) The computer-implemented method of claim 20 wherein the on-demand resource is computer hardware.

24. (Original) The computer-implemented method of claim 20 wherein the on-demand resource is selected from one of processors, memory and storage.

25. (Original) The computer-implemented method of claim 20 wherein validating the disablement code comprises verifying that the disablement code is unique to the on-demand resource.

26. (Original) The computer-implemented method of claim 20 wherein the validating comprises:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value, using the first key as an encryption key, to produce an encrypted value;

decrypting the encrypted value, using the decrypted data as a decryption key, to produce a decrypted value; and

comparing the value to the decrypted value.

27. (Original) The computer-implemented method of claim 20 wherein the validating comprises:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value, using the decrypted data as an encryption key, to produce an encrypted value;

decrypting the encrypted value, using the first key, to produce a decrypted value; and

comparing the value to the decrypted value.

28. (Original) The computer-implemented method of claim 27 wherein the decrypted data is identical to the first key.

29. (Original) The computer-implemented method of claim 27 wherein the decrypting is performed by a smart chip containing the second key.

30. (Original) The computer-implemented method of claim 27 wherein the encrypted data was encrypted using a copy of the second key at a remote location.

31. (Previously Presented) A computer-implemented method for generating disablement codes for disabling on-demand resources on a computerized apparatus, comprising:

inputting a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus;

outputting an authentication code;

encrypting the authentication code; and

providing a disablement code to a user of the computerized apparatus, the disablement code comprising the encrypted authentication code and being configured to disable an on-demand resource on the computerized apparatus upon being validated, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

32. (Original) The computer-implemented method of claim 31, further comprising selling the computerized apparatus to the user.

33. (Original) The computer-implemented method of claim 31, further comprising providing the computerized apparatus to the user with an installed instance of the authentication code generator.

34. (Original) The computer-implemented method of claim 31, further comprising providing the computerized apparatus to the user with an installed instance of the authentication code generator and a smart chip containing a unique key used to perform the encrypting of the authentication code.

35. (Original) The computer-implemented method of claim 31, wherein encrypting the authentication code is performed using a unique key stored in a secure storage element on the computerized apparatus, the secure storage element being inaccessible to a user of the computerized apparatus.

36. (Previously Presented) A computer readable medium containing a program which, when executed, performs an operation for generating disablement codes for disabling on-demand resources on a computerized apparatus, the operation comprising:

receiving a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus;

outputting an authentication code;

encrypting the authentication code; and

outputting a disablement code for the computerized apparatus, the disablement code comprising the encrypted authentication code and being uniquely configured to disable an on-demand resource on the computerized apparatus upon being validated, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

37. (Original) The computer readable medium of claim 36, wherein encrypting the authentication code is performed using a unique key stored in a secure storage element on the computerized apparatus, the secure storage element being inaccessible to a user of the computerized apparatus.

38. (Previously Presented) A computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus, the operation comprising:

receiving the disablement code comprising encrypted data; and

validating the disablement code, the validating comprising:

generating a first key using system information unique to the computerized apparatus;

sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key;

generating a random value;

encrypting the random value using the first key to produce an encrypted random value;

sending the encrypted random value to the secure storage element, wherein the secure storage element is configured to decrypt the encrypted random value, using the decrypted data as a decryption key, to produce a decrypted random value;

receiving the decrypted random value from the secure storage element; and

comparing the value to the decrypted random value.

39. (Original) The computer readable medium of claim 38, wherein the first key is identical to the decrypted data.

40. (Original) The computer readable medium of claim 38, wherein the secure storage element is a smart chip.

41. (Original) The computer readable medium of claim 38, wherein the on-demand resource was previously enabled to allow a user to request usage of the on-demand resource.

42. (Original) The computer readable medium of claim 38, further comprising disabling the on-demand resource, wherein the on-demand resource was previously enabled to allow a user to request usage of the on-demand resource and wherein disabling comprises preventing the user from requesting usage of the on-demand resource.

43. (Original) The computer-implemented method of claim 38 wherein the on-demand resource is a processor.

44. (Original) The computer-implemented method of claim 38 wherein the on-demand resource comprises one of memory and storage.

45. (Original) The computer-implemented method of claim 38 wherein the disablement code is input by a user.

46. (Previously Presented) A computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus, the operation comprising:

receiving the disablement code comprising encrypted data;

validating the disablement code, the validating comprising:

generating a first key using system information unique to the computerized apparatus;

sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key and further configured to encrypt a value using the decrypted data as an encryption key;

receiving the encrypted value from the secure storage element; and

decrypting the encrypted value using the first key; and

disabling the on-demand resources if the validating is successful, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

47. (Previously Presented) A computerized apparatus, comprising:

a plurality of resources at least one of which comprises an on-demand resource configured to be requested by a user once enabled; and

a capacity manager configured to at least:

receive an enablement code for the on-demand resource;

enable the on-demand resource;

receive a disablement code for the on-demand resource;

validate the disablement code; and

disable the on-demand resource, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus.

48. (Original) The computerized apparatus of claim 47, wherein the capacity manager is configured to validate the disablement code by encrypting and decrypting data.

49. (Original) The computerized apparatus of claim 47, wherein the capacity manager is configured to validate by verifying that the disablement code is unique to the on-demand resource.

50. (Original) The computerized apparatus of claim 47, wherein the on-demand resource comprises at least one of a processor, storage and memory.

51. (Original) The computerized apparatus of claim 47, wherein the capacity manager configured to enable by unlocking the on-demand resource and making the on-demand resource available for use upon request.

52. (Previously Presented) The computerized apparatus of claim 47, further comprising a user interface and wherein the capacity manager is further configured receive the enablement code and disablement code from the user.

53. (Original) The computerized apparatus of claim 47, wherein the capacity manager comprises a smart chip having an associated unique key.

# EVIDENCE APPENDIX

Copies of evidence submitted pursuant to 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and relied upon by appellant in the appeal, along with a statement setting forth where in the record that evidence was entered in the record by the examiner, are included as follows:

# RELATED PROCEEDINGS APPENDIX

Copies of decisions rendered by a court or the Board in the related appeal or interference listed on page 4 of this Brief are included as follows: